In the claims

Please add or amend the claims to read as follows and cancel without prejudice claims marked as cancelled:

1. **(Cancelled)**

2. **(Previously presented)** The system of claim 21 further comprising of a filtering module installed at the at least one server for blocking unauthorized processes in accordance with determined authorization level.

3. **(Previously presented)** The system of claim 21 further comprising at least one agent installed on the at least one server, said agent enables correlating between processes and sessions on different servers.

4. **(Currently amended)** The system of claim 21, wherein each the additional process comprises a process information vector, ~~wherein~~ and the module associates the ~~session ID~~ identification code of the original session ~~is added~~ to the additional process by adding the session identification code to the information vector of ~~each process in the sequence related to said original session~~the additional process.

5. **(Currently amended)** The system of claim 4 wherein the session identification code replaces redundant information in the process information vector.

6. **(Currently amended)** The system of claim 21 wherein the processes operated by each original session are associated to the original session's ~~session~~ identification code ~~ID~~ by a unique process identifier.

7. **(Currently amended)** The system of claim 21 wherein the ~~identified~~ original session properties are sign in parameters.

8. **(Currently amended)** The system of claim 21 wherein the ~~identified~~ original session properties are initial session type parameters.

9. **(Currently amended)** The system of claim 21 wherein the ~~identified~~ original session properties are hyperlink session address type parameters.

10. **(Previously presented)** The system of claim 21 wherein the original session is identified according to a unique Transmission Control Protocol (TCP) port ID.

11. **(Cancelled)**

12. **(Currently amended)** The method of claim 22 further comprising the step of filtering processes in accordance with the determined authorization level associated with the session ~~ID~~ identification code of each process.

13. **(Previously presented)** The method of claim 22 further comprising the step of correlating between process and sessions on different servers within the server network environment.

14. **(Currently amended)** The method of claim 22 wherein the process comprises a process information vector, and the association of the session ~~ID~~ identification code to the process ~~original session and its related processes includes~~ comprises ~~the step of~~ adding an identification code of the ~~identified communication~~ original session to the process information vector.

15. **(Previously presented)** The method of claim 14 wherein the identification code replaces redundant information in the process information vector.

16. **(Previously presented)** The method of claim 22 wherein the processes are associated to the original session by a unique process identifier.

17. **(Previously presented)** The method of claim 22 wherein the original session properties are sign in parameters.

18. **(Previously presented)** The method of claim 22 wherein the original session properties are initial session type parameters.

19. **(Previously presented)** The method of claim 22 wherein the original session properties are hyperlink session address type parameters.

20. **(Previously presented)** The method of claim 22 wherein the original session is associated with a unique Transmission Control Protocol (TCP) port ID.

21. **(Currently amended)** A security system ~~for real-time monitoring and controlling of communication sessions within a network server environment, wherein each original session enables operating a sequence of processes including operations carried out in the server environment,~~

~~said system~~ comprising:

~~at least one~~a server having an operating system, said server ~~enabling to~~ communicates with a multiplicity of client users via at least one communication network, wherein the client users initiate original sessions, each of which operates a sequence of processes, said sequence including one or more processes running on the operating system of the server, ~~wherein each client user enables accessing portals and operating sessions in the portals;~~ and

at least one module operated by said at least one server,

wherein said at least one module ~~enables~~ associates~~ing~~ a session ~~ID~~ identification code to ~~the~~ each original session ~~of the client user~~ and to each process in the sequence of processes operated by said original session, wherein said session ~~ID~~ identification code ~~enables determining an authorization level of session in accordance with predefined determination rules, wherein said determination rules refer to the properties of the original session, wherein each session ID~~ is related to the manner in which the client user has ~~operated~~ initiated the original session and is associated with an authorization level,

wherein ~~each process in the sequence is associated, in real time, with the same session ID of the original session, enabling said module to continuously monitor operation of~~

~~each process of each client user, while the at least one~~ the server ~~enables~~ operate~~s~~~~ing~~ the processes ~~of each original session~~ in the sequence of processes according to the authorization level ~~related to~~associated with the session ~~ID~~ identification code.

22. **(Currently amended)** A computer implemented method for ~~real-time~~ monitoring and controlling ~~of~~ communication sessions within a network server environment, wherein each original session ~~enables~~ operate~~s~~~~ing~~ a sequence of processes, ~~including operations carried out in the server environment,~~

said method comprising:

- associating each original session with a session ~~ID~~ identification code~~, wherein said session ID~~;
- associating the ~~session ID~~ identification code of the original session to each process in the sequence operated by the original session~~, in real time~~;
- ~~determining~~ associating an authorization level ~~related~~ to the session ~~ID~~ identification code in accordance with ~~predefined rules, wherein said rules refer to~~ the properties of the original session; and
- ~~continuously monitoring and~~ operating each process in the process sequence ~~associated with the original session,~~ according to the authorization level ~~related~~ associated to the session ~~ID~~ identification code~~, of each process~~

wherein said sequence of processes includes operations carried out in the operating system of the server.

23. **(New)** A security system comprising:

- a server, which communicates with a multiplicity of client users via at least one communication network, wherein the client users initiate communication sessions in one of specified manners, each of said communication sessions operates a

sequence of processes comprising one or more processes that operates an additional process; and

- at least one module which associates an ID to each communication session and to each additional process created by a process in the sequence of processes operated by said communication session,

wherein said ID is indicative of an authorization level,

wherein the authorization level is determined in accordance with the manner by which the communication session is initiated by the client user, and

wherein said server operates each additional process according to the authorization level indicated by the ID associated to the additional process by the module.

24. (New) A method of monitoring and/or controlling a communication session within a network server environment,

said method comprising:

- associating the communication session with a session identification code;
- associating an authorization level to the session identification code;
- associating the session identification code of the communication session at least to a child process, said child process been created by a process operated by the communication session; and
- operating the child process according to the authorization level associated with the session identification code.

25. (New) A method according to claim 24, wherein associating the session identification code to the child process comprises

- producing a hierarchical structure of processes at the kernel level; and

- referring each process to the hierarchical tree said each process belongs to.

26. (New) A method according to claim 24, wherein an authorization level is associated to the session identification code in accordance with the properties of the communication session.

27. (New) A security system according to claim 21, wherein one or more of said sequence of processes creates an additional process, and the additional process is associated with the session identification code.

28. (New) A method according to claim 22, wherein one or more of said sequence of processes creates an additional process, and the additional process is associated with the session identification code.